THE DIPLOMAT
Read The Diplomat, Know the Asia-Pacific

North Korea Is Still Trying to Hack US Critical Infrastructure

The ongoing cyber campaign seeks to infiltrate defense, financial, energy, telecom, and healthcare firms.

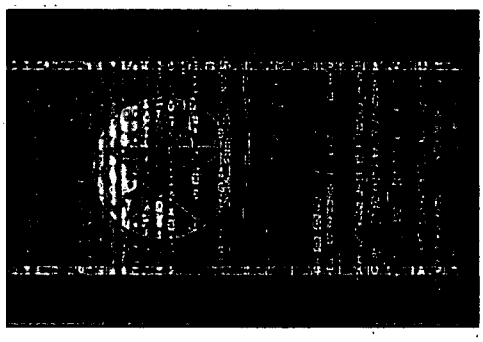

Image Credit: Illustration by Catherine Putz

By Troy Stangarone
March 14, 2019

While Donald Trump and Kim Jong Un were meeting in Hanoi to discuss the dismantlement of North Korea's nuclear weapons and ballistic missile programs, North Korea was also running a cyber operation to access critical infrastructure in the United States and other countries around the world.

The operation first became public in December 2018, when McAfee reported that a new global campaign had begun in October of that year designed to infiltrate defense, financial, energy, telecommunications, healthcare, and other firms. McAfee dubbed the effort Operation Sharpshooter.

At the time, Operation Sharpshooter was thought to have accessed critical systems in 87 companies, primarily in the United States. The attackers gained access to computer systems by sending phishing e-mails posing as job recruiters.

In its initial report, McAfee noted that there was evidence to suggest that North Korea was behind the operation. However, the technical links from Operation Sharpshooter to the Lazarus Group, a cybercrime group tied to North Korea and believed to be behind the Sony attack and the WannaCry ransomware attack, also seemed too obvious and raised concerns about a potential false flag operation designed to make it appear as though the Lazarus Group was behind the latest attacks.

New evidence, however, has more clearly linked the Lazarus Group to Operation Sharpshooter, which remains ongoing.

Thanks to an analysis of one of the command and control servers used in the attacks and provided by a government agency, McAfee has determined that Operation Sharpshooter likely dates back to September 2017, when the "fire and fury" standoff between the United States and North Korea was at its height. Not only has the operation been in place longer

than originally believed, but the scope of businesses and countries targeted is wider than originally known and the operation remains ongoing.

Cyber researchers, however, are perplexed by log files containing a batch of IP addresses from Namibia. But the idea of North Korea using Namibia for cyber operations may not be as odd as it seems on the surface. North Korea is known to run upwards of 200 hacker groups overseas using their work for trading companies as a cover, making the use of Namibia as a location for Pyongyang's hacking efforts a viable possibility.

In the case of Namibia, North Korea is known to have ties through the Korea Mining and Development Corporation and the Mansudae Overseas Projects, which provide military support to the Namibian government, including contracts for the construction of an arms and ammunition factory, military barracks, and a new headquarters for the Ministry of Defense.

The Namibian government has stated that its has cut its ties with North Korea as required by sanctions, but there are concerns that may not be the case.

Operation Sharpshooter isn't the only recent attempt by North Korea to access critical infrastructure. In 2018, McAfee also reported on a separate operation dubbed Operation GhostSecret, while FireEye identified efforts by APT37 to access a wide range of industries primarily in South Korea, but also the Middle East, Japan, and Vietnam.

Despite the ongoing talks with the United States to dismantle its nuclear weapons and missile programs, North Korea likely sees dual benefits in intelligence operations to probe critical infrastructure in the United States and around the world.

Should talks fail, access to critical infrastructure would give North Korea an additional way to retaliate against the United States in a future conflict.

North Korea is not the only country suspected of trying to gain access to U.S. critical infrastructure. In 2018, the U.S. Department of Homeland Security accused Russia of infiltrating the critical control systems of U.S. power plants, water, and electrical systems. While Russia has not manipulated power or shut down any U.S. critical infrastructure, Russian government-affiliated hackers are believed to be behind two large scale power outages in Ukraine in 2015 and 2016 and are believed to be engaged in continuing efforts to explore vulnerabilities in the U.S. power grid.

Access to critical systems could also serve as a means for the regime in Pyongyang to gain hard currency. U.S. Justice Department officials have noted that North Korea is increasingly turning to bank theft to make up for the loss of hard currency from sanctions. Not only are financial institutions known to be a target of Operation Sharpshooter, but data stolen from the targeted firms could potentially be monetized for hard currency as well.

The focus in talks with North Korea to date has largely been on its nuclear program, but we now know that the United States is also looking to dismantle Pyongyang's chemical and

biological weapons programs. North Korea's illicit cyber activities will likely be a topic for future discussions as well. However, if North Korea were to refuse to engage on the issue, the Trump administration would be required by law to maintain sanctions on North Korea for its cyber activities as part of the new Asia Reassurance Initiative Act until this issue has been resolved.
